EXHIBIT 2

10

From: Sieling, Lindsey (CHI) [/O=SKADDEN/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=LSIELING]
Sent: 10/31/2022 7:45:10 PM
To: 'Ahrens, Matthew' [MAhrens@crai.com]; 'Hardin, Bill' [BHardin@crai.com]; Ridgway, William (CHI) [/o=Skadden/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=WRIDGWAY8ad]
Subject: Dark web search
Attachments: Talking Points.pdf

Attached are talking points on Flagstar's ransomware attack, as well as the last four digits of SSN for the four individuals. It may take a couple days to get the email addresses from the client.

Saucedo: [redacted]
Angus: [redacted]
Smith: [redacted]
Robbins: [redacted]

Lindsey Sieling
Skadden, Arps, Slate, Meagher & Flom LLP
155 North Wacker Drive | Chicago | Illinois | 60606-1720
T: +1.312.407.0917 | **F: +1.312.827.9398**
lindsey.sieling@skadden.com

The Ransomware Attack

- In late November and early December 2021, Flagstar identified suspicious activity on its network, which it later identified to be part of a ransomware attack.
- Flagstar promptly initiated its incident response protocol and took steps to address the incident, including partnering with Kroll to remediate and investigate the situation.
- Flagstar's systems have since been secured, and all unauthorized access has been revoked since December 2021, which Kroll has independently verified.
- Flagstar notified law enforcement and the OCC. Flagstar has been providing the OCC periodic updates throughout the investigation and remediation.
- Flagstar's investigation revealed the following:
  - The earliest evidence of unauthorized activity in its environment occurred on November 22, 2021, when a threat actor exploited the credentials of a contractor.
  - The threat actor is associated with the "Shao" ransomware group.
  - The threat actor exfiltrated data from some of the Bank's servers on December 3 and 4, 2021.
  - The threat actor also used distributed denial of service (DDOS) attacks and was successful in encrypting certain data in the Bank's network, which caused some interruption to its operations.
  - Flagstar was able to restore its systems promptly using backup servers, which were not impacted by the incident.
- Kroll is currently reviewing the exfiltrated data, among other things, to determine the nature and extent of exfiltrated PII.
- In coordination with its insurance carrier, Flagstar made a payment to the threat actors on December 31, 2021, to further reduce risk associated with this incident, including to delete the exfiltrated data from the threat actor's servers. The amount of the payment is not material to Flagstar and is expected to be reimbursed by its insurance carrier.
- Flagstar's security vendors continue to monitor the dark web, including the site associated with the "Shao" ransomware group, and have identified no evidence that the threat actors have released any Flagstar data.
- Upon completion of Kroll's review, Flagstar will make required notifications to customers and regulators and offer appropriate customer protections, such as credit monitoring services.

- Flagstar does not believe the Ransomware Attack will have a material adverse impact on its business, results of operations, or financial condition.